

IBM Trusteer Pinpoint Assure

Nella presente Descrizione dei Servizi viene illustrato il Servizio Cloud. I documenti di ordine applicabili forniscono prezzi e dettagli aggiuntivi sull'ordine del cliente.

1. Servizio in Cloud

IBM Trusteer Pinpoint Assure è una soluzione stratificata orientata alla sicurezza, appositamente progettata per impedire a persone con intento fraudolento di utilizzare identità rubate, aggiungere dati falsi ad identità reali o creare identità fasulle da utilizzare per effettuare una transazione guest, aprire un nuovo account o aprire un nuovo account digitale per conto di un cliente esistente.

1.1 Offerte

1.1.1 IBM Trusteer Pinpoint Assure

Questo servizio contrassegna le attività sospette e genera degli avvisi durante il processo di creazione/generazione di un nuovo account. Il servizio controlla il processo di registrazione dell'account per identificare le attività fraudolente, in modo da avvisare tempestivamente che il nuovo account potrebbe essere di tipo mule o utilizzato a scopo fraudolento, tramite report di utilizzo disponibili in Trusteer Management Application (TMA). Come parte del processo di login di TMA vengono utilizzati IBM Trusteer Pinpoint Detect e IBM Trusteer Pinpoint Verify.

IBM Trusteer Pinpoint Assure è disponibile in pacchetti di 100 Connessioni annuali.

1.2 Servizi Opzionali

1.2.1 IBM Trusteer Pinpoint Assure Application

Per la distribuzione di IBM Trusteer Pinpoint Assure su qualsiasi Applicazione è richiesta la titolarità per IBM Trusteer Pinpoint Assure Application.

Il servizio IBM Trusteer Pinpoint Assure è disponibile per l'acquisto in base all'applicazione.

1.2.2 IBM Trusteer Mobile Carrier Intelligence

Il Cliente deve disporre di un abbonamento attivo a IBM Trusteer Pinpoint Assure prima di abbonarsi al presente Servizio Cloud.

Il presente Servizio Cloud migliora IBM Trusteer Pinpoint Assure fornendo ulteriori informazioni e contesto sui numeri di cellulare forniti ai Servizi Cloud, consentendo di determinare il rischio di frode di una determinata sessione. Il Cliente potrà interrogare il Servizio Cloud per determinare le caratteristiche di un numero di cellulare specifico, quali ad esempio le informazioni sul gestore telefonico associate a tale numero.

I dati forniti da questo Servizio Cloud relativi ai numeri di cellulare ("Mobile Intelligence") possono essere utilizzati solo per scopi interni del Cliente e possono essere conservati per un periodo di 30 (trenta) giorni. Dopo tale periodo di tempo il Cliente dovrà interrogare nuovamente il Servizio Cloud per lo stesso numero di cellulare per ottenere la "Mobile Intelligence" ad esso relativa e non potrà semplicemente riutilizzare la "Mobile Intelligence" ricevuta da una query precedente. Salvo per quanto sopra consentito il Cliente non potrà memorizzare nella cache, riutilizzare, utilizzare in modo congiunto completo o parziale con qualsiasi data mining, o archiviare alcuna Mobile Intelligence.

2. Specifiche Tecniche per la Protezione e il Trattamento dei Dati (Data Processing and Protection Data Sheets)

Il Supplemento al Trattamento dei Dati Personali (DPA o Data Processing Addendum) di IBM, disponibile alla pagina web <http://ibm.com/dpa> e le Specifiche Tecniche per la Protezione e il Trattamento dei Dati (Data Sheet o Appendice DPA) nei seguenti link forniscono ulteriori informazioni sulla protezione dei dati per i Servizi Cloud e per le opzioni relative ai tipi di Contenuto che potrebbe essere trattato, per le attività di trattamento interessate, le funzionalità per la protezione dei dati e le specifiche sulla conservazione e restituzione del Contenuto. Il DPA si applica ai dati personali presenti nel Contenuto, nella misura in cui si applichino i) il Regolamento Europeo in materia di Protezione dei Dati Personali (European General Data

Protection Regulation, EU/2016/679, GDPR); o ii) altre leggi sulla protezione dei dati riportate alla pagina <http://ibm.com/dpa/dpl>.

Le Specifiche Tecniche solitamente riportano tutte le sedi in cui IBM (compreso qualsiasi subresponsabile di terze parti) ospita e tratta i Dati Personali, senza considerare il data center da cui vengono erogati i servizi. Per un elenco delle sedi di hosting e trattamento specifiche del data center da cui vengono erogati i servizi, consultare l'Articolo 5.1 riportato di seguito (Ulteriori Informazioni sulla Sede del Trattamento).

IBM Trusteer Assure

<https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=CF0C527046E011E8ADCBA344DE8FB657>

IBM Trusteer Mobile SDK

<https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=1402492847439>

3. Livelli di Servizio e Supporto Tecnico

3.1 Service Level Agreement ("SLA")

IBM fornisce al Cliente il seguente Service Level Agreement ("SLA"). IBM applicherà il Rimborso più elevato applicabile sulla base della disponibilità cumulativa del Servizio Cloud raggiunta, come mostrato nella tabella seguente. La percentuale di disponibilità viene calcolata nel seguente modo: il numero totale di minuti nel mese contrattuale, meno il numero totale di minuti di Inattività del Servizio nel mese contrattuale, diviso per il numero totale di minuti nel mese contrattuale. La definizione di Inattività del Servizio, il processo di reclamo e le modalità per contattare IBM in relazione ai problemi di disponibilità del servizio sono riportati nel manuale di supporto al Servizio Cloud di IBM all'indirizzo https://www.ibm.com/software/support/saas_support_overview.html.

Disponibilità	Credito (% della quota di abbonamento mensile*)
Inferiore al 99,9%	2%
Inferiore al 99,0%	5%
Inferiore al 95,0%	10%

* La quota di abbonamento rappresenta il prezzo contrattuale per il mese soggetto al reclamo.

3.2 Supporto tecnico

Il supporto tecnico per il Servizio Cloud, inclusi i dettagli di contatto di assistenza, i livelli di gravità, le ore di disponibilità del supporto, i tempi di risposta e altre informazioni e processi relativi al supporto, possono essere consultati selezionando il Servizio Cloud nella guida di supporto IBM disponibile alla pagina <https://www.ibm.com/support/home/pages/support-guide/>.

4. Corrispettivi

4.1 Calcolo dei Corrispettivi

Le metriche dei corrispettivi per il Servizio Cloud sono specificate nel Documento d'Ordine.

Al presente Servizio Cloud si applica il seguente calcolo dei corrispettivi:

- Una Connessione è un collegamento o l'associazione di un database, un'applicazione, un server o di qualsiasi altro tipo di dispositivo, che è o è stato reso disponibile al Servizio Cloud.
- Per Applicazione si intende un programma software denominato in modo univoco, fornito o reso disponibile, per accedere ai Servizi Cloud o da questi utilizzato.

5. Ulteriori condizioni

Agli Accordi per i Servizi Cloud (o agli accordi equivalenti per il cloud di base), stipulati prima del 1 gennaio 2019, si applicano le condizioni riportate alla pagina web <https://www.ibm.com/acs>.

5.1 Ulteriori Informazioni sulla Sede del Trattamento

Tutto l'hosting ed il trattamento dei dati personali, compresi da tutti i subresponsabili di terze parti identificati nelle Specifiche Tecniche, sarà condotto in tutte le sedi indicate di seguito:

Per tutti i servizi forniti tramite i data center ubicati in Germania, IBM limiterà l'hosting ed il trattamento dei Dati Personali al paese dell'entità appaltante di IBM ed ai seguenti paesi: Germania, Israele, Irlanda e Paesi Bassi.

Per tutti i servizi forniti tramite i data center ubicati in Giappone, IBM limiterà l'hosting ed il trattamento dei Dati Personali al paese dell'entità appaltante di IBM ed ai seguenti paesi: Giappone, Israele ed Irlanda.

Per tutti i servizi forniti tramite i data center ubicati negli Stati Uniti, IBM limiterà l'hosting ed il trattamento dei Dati Personali al paese dell'entità appaltante di IBM ed ai seguenti paesi: Stati Uniti, Israele, Irlanda, Singapore ed Australia.

Oltre alle sedi riportate in precedenza, per tutti i servizi forniti tramite i data center siti in Germania, Giappone e Stati Uniti, (1) l'hosting ed il trattamento dei dati di supporto potrà essere assicurato in Germania e Francia da Salesforce.Com, in qualità di subresponsabile di terze parti e (2) per i clienti con l'opzione che consente di inviare dati ai provider Mobile Carrier Intelligence, l'hosting ed il trattamento dei Dati Personali potrà avvenire nei paesi dei subresponsabili di terze parti applicabili, come riportato nelle Specifiche Tecniche. Nonostante quanto diversamente indicato nelle Specifiche Tecniche, i subresponsabili di terze parti specificati nella clausola (2) della frase precedente potrebbero non essere conformi a ISO 27001 o SOC2.

I servizi di manutenzione dell'account e di supporto IBM Trusteer possono anche essere forniti secondo le necessità, in base alla disponibilità del personale IBM rilevante, alla posizione del Cliente ed al data center che ospita i dati.

5.2 Soluzioni integrate

Per chiarezza, le diverse offerte con marchi Trusteer possono costituire una soluzione integrata. Pertanto, se il Cliente recede da uno di questi Servizi Cloud, IBM potrà conservare i dati del Cliente allo scopo di assicurare l'erogazione al Cliente dei rimanenti Servizi Cloud, in base alla presente Descrizione dei Servizi, oltre ad altri servizi Trusteer, ai sensi delle descrizioni dei servizi applicabili a tale altro servizio Trusteer.

5.3 Dati raccolti come parte della distribuzione

La distribuzione del Servizio Cloud può comportare la fornitura a IBM di determinati dati da parte del Cliente. Tali dati non devono includere informazioni che possono identificare o che possono essere attribuite a individui specifici. Ulteriori Linee Guida sui dati forniti a IBM come parte della distribuzione, sono incluse nelle Linee Guida sulla Distribuzione di Trusteer, da fornire al Cliente.

6. Condizioni derogative

6.1 Uso dei Dati

Quanto segue prevale su quanto diversamente riportato nell'Articolo Contenuto e Protezione dei Dati Personali dei termini di base del Servizio Cloud tra le parti: IBM non utilizzerà o divulgherà i risultati derivanti dall'utilizzo da parte del Cliente del Servizio Cloud che sono specifici del Contenuto del Cliente (Approfondimenti) o che altrimenti identifichino il Cliente. IBM tuttavia utilizzerà il Contenuto e altre informazioni derivanti dal Contenuto (ad eccezione degli Approfondimenti), come parte del Servizio Cloud, allo scopo di migliorare il Servizio Cloud. Allo scopo di migliorare il processo di rilevamento delle minacce e la conseguente protezione dalle stesse, IBM potrà decidere di condividere gli identificatori di minacce ed altre informazioni di sicurezza presenti nel Contenuto.

Accettato da:

Firma e timbro del Cliente

Data:

Ai sensi e per gli effetti degli articoli 1341 e 1342 del Codice Civile Italiano, il Cliente approva specificamente i seguenti articoli del presente documento: "Specifiche Tecniche per la Protezione e il Trattamento dei Dati (Data Processing and Protection Data Sheets)", "Service Level Agreement ("SLA")".

Accettato da:

Firma e timbro del Cliente

Data: